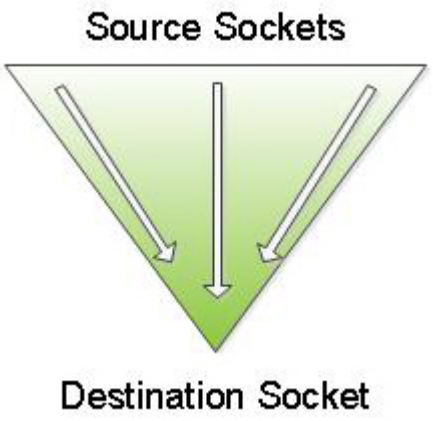
SYN-Ack Flood Attack - Corero

What is a SYN-ACK Flood Attack?



Attack Description:

In an **ACK DDoS attack** (or ACK-PUSH Flood), attackers send spoofed ACK (or ACK-PUSH) packets at very high packet rates that fail to belong to any current session within the firewall's state-table and/or server's connection list. Typically, a smaller botnet sends spoofed SYN packets to large numbers of servers and proxies on the Internet that generate large numbers of SYN-ACK packets in response to incoming SYN requests from the spoofed attackers. This SYN-ACK flood is not directed back to the botnet, but instead, is directed back to victim's network and often exhausts the victim's firewalls by forcing state-table lookups for every incoming SYN-ACK packet. This denial of service attack can render stateful devices inoperable and can also consume excessive amounts of resources on routers, servers and IPS/IDS devices.

The ACK flood exhausts a victim's firewalls by forcing state-table lookups and depletes server resources used to match these incoming packets to an existing flow.

HOW TO PROTECT AGAINST SYN-ACK FLOOD:

During a DDoS attack, a firewall is easily compromised, offering no defense to servers downstream. Corero's technology blocks the bad traffic and allows all normal/good traffic to pass through.

Additional & Related Information:

- SYN Flood
- Frequently Asked Questions About DDoS Attacks
- On-Premises Defense Against SYN-ACK Flood Attacks